#14

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPELLANT:	Frank Reisinger	CONFIRMATION NO. 4346
SERIAL NO.:	09/340,782	GROUP ART UNIT: 3621
FILED:	June 28, 1999	EXAMINER: C. Sherr
TITLE:	"METHOD FOR THE DEPENDABLE TRANSMISSION SERVICE DATA TO A TERMINAL EQUIPMENT AND ARRANGEMENT FOR IMPLEMENTING THE METHOD"	

Assistant Commissioner for Patents,

Washington, D.C. 20231

APPELLANT'S APPEAL BRIEF

S I R:

Pursuant to 37 C.F.R. §1.192, Appellant herewith submits his main Brief in the appeal of the above-referenced application.

REAL PARTY IN INTEREST:

The real party in interest is the assignee of the application, Francotyp-Postalia AG & Co. KG, a German corporation.

RELATED APPEALS AND INTERFERENCES:

There are no related appeals and no related interferences.

STATUS OF CLAIMS:

Claims 1-32 are on appeal, and constitute all of the original claims of the application. No claim has been cancelled during prosecution.

STATUS OF AMENDMENTS:

No Amendment has been filed following the final rejection dated October 29, 2002.

SUMMARY OF THE INVENTION:

The method and apparatus of the claims on appeal can be practiced in embodiments as shown in Figure 1a and 1c employing a microprocessor 6 as a control unit, or in an embodiment as shown in Figure 1b, employing a one-time programmable (OTP) processor 6 as the control unit. The basic components and method steps in these different embodiments do not significantly differ, and therefore the embodiment employing a microprocessor will be described below, for simplicity and to avoid duplication.

In general, the method and apparatus which are the subject of the claims on appeal are for the purpose of determining when the contents of a usage memory, wherein usage data are accumulated during the operation of a device, are to be transferred to a remote location for analysis, such as a statistical analysis. Since the primary intended use of the apparatus and method of the claims on appeal is a postage meter, which is a relatively small device having limited memory capacity, the method and apparatus of the claims on appeal make use of monitoring the remaining memory contents of the memory in which the usage data are stored as the criterion for data transfer to the remote location for analysis.

Figure 1a shows a block circuit diagram of the inventive postage meter machine with a printer module 1 for a completely electronically generated franking image. This postage meter machine has at least one input unit 2 with a number of actuation elements, a display unit 3, a modem 23 that produces the communication with a data center. A further input unit 21 and/or a scale 22 is/are coupled to a control unit 6 via an input/output control module 4. The postage meter machine has non-volatile memories 5a, 5b, 9, 10 and 11 for data that contain the variable or the

constant parts of the franking image and programs for processing the data in conjunction with the mail carrier and service to be carried out by the carrier (as explained below). (p.7, l.14-22)

Obtaining the postage fee schedule table data from the data center ensues as needed or in conjunction with the remote loading of the postage meter machine with a credit (postage call for the purpose of re-crediting), with the security measures of the credit loading being utilized also for the table loading. (p.9, l.3-6) The postage fee schedule table data are initially intermediately stored in the memory area 7d of the volatile main memory RAM 7 of the postage meter machine. (p.9, l.6-8) The microprocessor 6 can now form a checksum over the content of the postage fee schedule table data and send this checksum by modem 23 to the data center DZ land-line or radio via a communication network. (p.9, l.8-11) The data center DZ has a modem 33 that is connected to a server 32 that accesses a data bank 31. (p.9, l.11-12) The requesting postage meter machine identifies itself at the data center with its PIN (postage call identification number) and communicates the version number for the purpose of locating a new postage fee schedule table in the data bank DB31 of the data center, wherein a postage fee schedule table is allocated to the communicated version number. (p.9, l.12-16) The server 32 is programmed for checking the proper transmission and error-free intermediate storage of service data on the basis of the checksum, as will be explained in yet greater detail with reference to Figures 3a and 3b. (p.9, l.16-18)

When a modified postage fee schedule table is required in an electronic postage computer, a remote installation can ensue on demand. A postage fee schedule table is to be communicated to the terminal equipment on demand in order

to be able to load this into corresponding memories of the postage computer. (p.10, l.10-13) Given such a remote installation, one embodiment of the inventive method for dependable transmission of service data to a terminal equipment proceeds according to the following method steps:

In step 210 as shown in Fig. 2, new postage fee schedule table data are offered in the data center for a future postage calculation. (p.10, l.13-17) In step 110 the terminal equipment (postage calculator) formulates request data for postage fee schedule table data. (p.10, l.17-18) In a first communication 120 of the terminal equipment with the data center, the request data are transmitted in order to request the new postage fee schedule table data from the data center, and comprising a reception and storing of the requested postage fee schedule table data are subsequently received and stored by the terminal equipment. (p.10, l.18-22) In a first communication 220 of the data center with the terminal equipment, the aforementioned request data are received at the data center and the requested postage fee schedule table data are transmitted to the terminal equipment. (p.10, l.22 - p.11, l.2) In a second communication 130 of the terminal equipment with the data center, a message is formed at the terminal equipment and is communicated to the data center, that refers to the stored, valid, new postage fee schedule table data. (p.11, l.2-5) In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and an OK message is transmitted to the terminal equipment, and in step 240 a registration of the service performed ensues in the data center in conjunction with the transmission of an OK message. (p.11, l.5-10)

Upon reception of the OK message in the terminal equipment, an indicator that the stored data is registered in valid form ensues and a flag for payment of the service ensues in the data center. As the indicator, either a bit is set in a secured area in the non-volatile memory of the postage computer or corresponding MAC-protected data are stored. The microprocessor only utilizes data registered as valid for calculating postage. (p.11, l.11-16)

The following method steps proceed in an alternative embodiment:

In step 210, new postage fee schedule table data are offered in the data center for a future postage calculation. (p.11, l.17-19) In step 110 the terminal equipment (postage calculator) formulates request data for postage fee schedule table data. (p.11, l.19-20) In a first communication 120 of the terminal equipment with the data center, the request data are transmitted in order to request the new postage fee schedule table data from the data center, and comprising a reception and storing of the requested postage fee schedule table data are subsequently received and stored by the terminal equipment. (p.11, l.19 - p.20, l.1) In a first communication 220 of the data center with the terminal equipment, the aforementioned request data re received at the data center and the requested postage fee schedule table data are transmitted to the terminal equipment. (p.12, l.1-4) In a second communication 130 of the terminal equipment with the data center, a message is formed at the terminal equipment and is communicated to the data center, that refers to the stored, valid, new postage fee schedule table data. (p.12, l. 4-7) In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table

data, and an OK message is transmitted to the terminal equipment, and in step 240 a registration of the service performed ensues in the data center in conjunction with the transmission of an OK message. (p.12, l. 7-12)

In a second communication 230 of the data center with the terminal equipment, the aforementioned message is received by and checked in the data center by comparison information generated from the postage fee schedule table data, and a load instruction is transmitted to the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of its postage computer. (p.12, l. 13-17)

A registration (step 240) of the loading ensues in the data center, and loading (step 140) of the postage fee schedule table data into a non-volatile memory of the postage computer ensues after reception of the load instruction. (p.12, l. 18-20)

Figures 3a and 3b show first and second versions of a flowchart for checking the dependable transmission of data to the terminal equipment. (p.17, l.8-9)

In one version, shown in Figure 3a, the encrypted checksum is formed by the postage computer on the basis of an asymmetrical encryption algorithm, a public key being stored therein, and an appertaining, private, secret key (PRIVATE KEY) is employed for checking in the data center, this being stored in a secure manner and being kept secret from third parties. (p.17, l.10-14) Given an RSA signature, a message based on the version number and on the checksum is encrypted with a public write key (PUBLIC KEY) to form a digital signature. (p.17, l.14-16) The digital signature (SIGNATURE) is sent from the terminal equipment to the data center together with the identification number PIN and the version number (VERSION NO), the data center being capable of decrypting the signature with a secret read key

(PRIVATE KEY) according to the asymmetrical algorithm (RSA). (p.17, l.16-20) The checksum (CHECK SUM) over the content of the fee schedule table data that are stored in the data bank 31 allocated to the version number (and possibly also allocated to the PIN) must agree with the decrypted message if the fee schedule table data intermediately stored in the postage computer or in the postage meter machine are to be recognized as being valid. (p.17, l.20 - p.18, l.1) This verification is a prerequisite in order to communicate a corresponding command to the postage meter machine. (p.18, l.1-2) The rate table check sum formation can ensue before or during the communication. (p.18, l.3) A prior formation has the advantage that the comparison check sum RATE TABLE CHECK SUM is stored in the data bank 31 allocated to the version number VERSION NO. or PIN and can be called directly from the data bank 31 by the server 32 for comparison. (p.18, l.3-7) The calculating time of the server 32 that is saved is thus advantageously available to the decryption procedure of the SIGNATURE. (p.18, l.7-8) The decrypted message is identical to the checksum CHECK SUM that was formed in the postage computer or terminal equipment from the volatilely intermediately stored postage fee schedule table. (p.18, l.8-10) Given proper intermediate storage, the decrypted checksum CHECK SUM is identical to the comparison checksum RATE TABLE CHECK SUM that is formed or stored in the data bank 31. (p.18, l.11-13)

In another version, shown in Figure 3b, an encrypted checksum MAC (message authentication code) is formed with a symmetrical encryption algorithm, this being formed by the postage meter machine in which a secret key is stored. (p.18, l.18-20) The encrypted checksum MAC is communicated to the data center. (p.18, l.20-21)Differing from the version shown in Figure 3a, no decryption is

implemented in the data center; rather, an encryption is implemented in order to encrypt a checksum derived from the postage fee schedule table to form a comparison MAC=. (p.18, l.21 - p.19, l.1) The RATE TABLE CHECK SUM formation can ensue before or during the communication. Such a prior formation has the advantage that the CHECK SUM merely has to be called from the data bank 31 in order to generate the comparison MAC= from this CHECK SUM by encryption with a secret key SECRET KEY using a symmetrical algorithm DES with the assistance of the server 32: (p.19, l.2-5)

The same secret key SECRET KEY is employed in the check in the data center as in the postage meter machine. (p.19, l.6-7) The check in the data center preferably ensues with both MACs. (p.19, l.7-8) A suitable version of the DES algorithm is preferably utilized in the MAC formation. (p.19, l.8-9) The same secret DES key is employed given a MAC formation in the data center and in the postage meter machine. (p.19, l.9-10) To that end, the secret DES key must be stored secured in the data bank 31 allocated to that PIN identifying the terminal equipment. (p.19, l.10-12) Alternatively, the RATE TABLE CHECK SUM formation and the encryption to form a comparison MAC can ensue in common before the communication. (p.19, l.12-13) The comparison MAC is then stored in the data bank 31 allocated to the PIN and to the version number and can be called by the server for comparison purposes. (p.19, l.13-15)

ISSUES:

The issues on appeal are as follows:

Whether the subject matter of claims 1-11 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on

the teachings of United States Patent No. 4,752,950 (Le Carpentier) in view of the teachings of United States Patent No. 5,715,164 (Liechti et al.);

Whether the subject matter of claims 12-16 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of Le Carpentier in view Liechti et al;

Whether the subject matter of claims 17-27 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of Le Carpentier in view of Liechti et al.; and

Whether the subject matter of claims 28-34 would have been obvious to a person of ordinary skill in the art under the provisions of 35 U.S.C. §103(a) based on the teachings of Le Carpentier in view of Liechti et al.

GROUPING OF CLAIMS:

The claims on appeal include independent method claims 1 and 12 and independent apparatus claims 17 and 28. Of those independent claims, the patentability of claims 1 and 17 stands or falls together and the patentability of claims 12 and 28 stands or falls together. The patentability of claims 1 and 17 does not stand or fall together with the patentability of claims 12 and 28.

Of the dependent claims, claims 2-11 depend from claim 1. Separate arguments in support of the patentability of claims 2-11 are set forth below, and therefore the patentability of claims 2-11 does not stand or fall together with the patentability of independent claim 1. The patentability of claims 2-11 stands or falls together.

Claims 13-16 depend from claim 12, and separate arguments are set forth below in support of the patentability of claims 13-16. The patentability of claims 13-

16 therefore does not stand or fall together with the patentability of claim 12. The patentability of claims 13-16 stands or falls together.

Claims 18-27 depend from claim 17 and separate arguments are set forth below in support of the patentability of claims 18-27. The patentability of claims 18-27 therefore does not stand or fall together with the patentability of claim 17. The patentability of claims 18-27 stands or falls together.

Claims 29-32 depend from claim 28. Separate arguments in support of the patentability of claims 29-32 are set forth below, and therefore the patentability of claims 29-32 does not stand or fall together with the patentability of claim 28. The patentability of claims 29-32 stands or falls together.

ARGUMENT:

As alleged substantiation for the aforementioned rejections, the Examiner has merely copied various claim elements and has followed each of those claims elements with a column and line citation from the Le Carpentier or :Liechti et al. references. The Examiner did not make any effort to demonstrate how the cited passage allegedly corresponds to the claim language, and in most instances there is virtually no resemblance whatsoever between the reference passage cited by the Examiner and the claim language of the present application. Simply providing such citations with no further explanation is not a proper basis for substantiating a rejection under 35 U.S.C. §103(a) and therefore, as a generalized argument, Appellant respectfully submits the Examiner has failed to establish a *prima facie* case of obviousness for any of claims 1-32.

In the final rejection, in response to the aforementioned argument, the Examiner stated that as long as a rejection takes into account only knowledge which

was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the Appellant's disclosure, such a reconstruction is proper. Appellant of course has no disagreement with this general statement of the law, however, even this general criterion is not satisfied by merely repeating the claim language and providing citations to various passages in prior art references, without any effort to demonstrate why the cited passages allegedly correspond to the claim language. This is particularly true when, as here, Appellant has provided extensive discussion and analysis in support of Appellant's position that the reliance by the Examiner on the cited passages is incorrect with regard to their content and/or the alleged correlation between those passages and the claim language. In response to these arguments of the Appellant made during prosecution, the Examiner merely repeated the citations in the references (which are discussed in detail below), but did not provide any refutation or commentary regarding Appellant's arguments as to why those citations are inappropriate for supporting a rejection under 35 U.S.C. §103(a). Appellant at this time, therefore, is still unable to determine how or why the Examiner refutes Appellant's arguments.

Moreover, after providing these citations to various passages in the prior art references, the Examiner has merely alleged that it would have been obvious to a person of ordinary skill in the art to modify one or both of the references, but has not substantiated that allegation with any evidence. Appellant acknowledges that an explicit suggestion to combine or modify references is not necessary in order to support a rejection under 35 U.S.C. §103(a), and also acknowledge that the references always must be considered as a whole. Nevertheless, this does not alleviate the obligation on the part of the Examiner to substantiate the rejection with

something more than a mere allegation that such motivation or suggestion exists. As stated by the Federal Circuit in *In re Kotzab,* 54 U.S.P.Q. 2d 1308, 1316 (Fed. Cir. 2000):

> [T]o establish obviousness based on a combination of the elements disclosed in the prior art, there must be some motivation, suggestion or teaching of the desirability of making the specific combination that was made by the applicant.

The Federal Circuit further stated in *In re Dembiczak*, 50 U.S.P.Q. 2d 1614, 1617 (Fed. Cir. 1999):

> Our case law makes clear that the best defense against the subtle but powerful attraction of a hindsight-based obviousness analysis is a *rigorous* application of the requirement for a showing of the teaching or motivation to combine prior art references. (Emphasis added)

Further, in *In re Mayne,* 41 US.P.Q.2d 1451, 1454 (Fed. Cir. 1997), the Federal Circuit stated:

> When relying on numerous references or a modification of prior art, it is incumbent upon the Examiner to identify some suggestion to combine the references or make the modification.

Additionally in the *In re Dembiczak* Decision noted above, the Federal Circuit stated:

> We have noted that evidence of a suggestion, teaching, or motivation to combine may flow from the prior art references themselves, the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved, ... The range of sources available, however, does not diminish the requirement for actual evidence. That is, the showing must be clear and particular. ...Broad conclusory statements regarding the teaching of multiple references, standing alone, are not "evidence."

Turning more specifically to the content of the claims, independent claim 1 of the present application, as a first step, requires that new service data be offered at a data center for future use at terminal equipment. The terminal equipment then formulate a request for the new service data, and a first communication is

established between the terminal equipment and the data center, wherein the request data are transmitted from the terminal equipment to the data center.

The Examiner has characterized column 2, lines 17-24 in the Le Carpentier reference as teaching a method for dependably transmitting service data from a data center to remotely located terminal equipment, including the step of offering new service data at the data center for future use at the terminal equipment. This passage, however, is merely a generalized statement regarding "control" of a plurality of franking machines from a central station, and says nothing whatsoever regarding new service data. In fact, virtually the entirety of the Le Carpentier reference is directed to *interrogating* the franking machines by a local station that is in turn in communication with the central station. Obviously such interrogation involves an interrogation request *from* the local station *to* the franking machine, followed by transmission of stored data *from* the franking machine *to* the local station. Only in column 9 of the Le Carpentier reference is any mention whatsoever made of data transmission in the opposite direction, i.e., *from* the local station (or the central station) *to* the franking machine. This, however, involves initialization of the franking machine which, as is known to those of ordinary skill in the art, involves the so-called "commissioning" of the franking machine whereby all of the data necessary for an initial start-up of the franking machine are transmitted. Obviously, prior to this time, the franking machine is not in use, and cannot be in use, and therefore such initialization cannot involve any transmission of any sort in the opposite direction, in the form of a request or otherwise.

The Examiner cited language at column 4, lines 49-53 as allegedly teaching "forming a request for new service data at the terminal equipment." This passage in

the Le Carpentier reference, however, does not refer to communication between the franking machine and the local station (or the central station) but refers to an exchange of data between the franking head and the base 7 of the franking machine. This communication routine is necessary because the base 7 must be able to "recognize" that a particular franking head is in place and therefore a type of "handshake" routine must be executed each time the franking machine is turned on. If the base 7 recognizes that a changed franking head is in place, operation of the franking machine is temporarily inhibited until it can be assured that the new franking head is authorized. In any event, this exchange does not involve any sort of request, and particularly does not involve a request for new service data; it is merely an exchange of existing information.

The Examiner also cited the language at column 4, lines 49-63 in the Le Carpentier reference as allegedly teaching the other sub-steps of the first communication, however, as noted above it is clear that this passage is referring to a data exchange between the base 7 and the franking head, and does not involve the data center or the local station whatsoever.

The Examiner then cited language at column 5, lines 1-15 of the Le Carpentier reference as allegedly teaching establishment of a second communication between the terminal equipment and the data center. This communication is, in fact, a communication between the base 7 and the local station, however, since the aforementioned data exchange took place between the base 7 and the franking head, this is not a "second communication between the terminal equipment and the data center" but is in fact only the first such communication. Moreover, the claim language requires that the terminal equipment form a message

referring to the new service data and communicate this message from the terminal equipment to the data center. The passage cited by the Examiner proceeds precisely oppositely, because it is initiated by a request from the local station, which results in a response from the base in the form of a message. Moreover, although this message that is sent from the base to the local station is encrypted, there is no teaching whatsoever in the passage cited by the Examiner that the encryption has anything to do with, or is in any way based on, the request from the local station. The claim language, by contrast, requires that the message sent from the terminal equipment to the data center refer to the new service data stored at the terminal equipment. Moreover, as noted above the only information transmitted from the terminal equipment in response to such a request consists of compiled usage data, identified by an identification number, relating to usage of the terminal equipment. The transmitted information has nothing to do with "new service data."

The Examiner also cited this passage at column 5, lines 1-15 as teaching the transmission of a follow-up message from the data center to the terminal equipment, however, Appellant and his counsel are unable to find any statement whatsoever in this passage remotely resembling a teaching to transmit a follow-up message from the data center to the terminal equipment after the terminal equipment has transmitted data to the data center (or local station) in response to the aforementioned request from the local station.

The Examiner also cited this language as teaching that the follow-up message is an "OK message" allowing the terminal equipment to be switched to an operating mode, however, Appellant is unable to find any teaching whatsoever that the data exchange described at column 5, lines 1-15 of the Le Carpentier reference has

anything whatsoever to do with switching the terminal equipment to an operating mode. In fact, it appears that the terminal equipment already is, and must be, in an operating mode in order to even participate in the data exchange described at column 5, lines 1-15 of Le Carpentier.

In view of the procedure adopted by the Examiner of providing line and column citations following a recitation of the language of the claims in question, it appears that the Examiner relied solely on the Le Carpentier reference as a basis for rejecting independent claim 1, and did not rely on any teachings of the Liechti et al. reference with regard to claim 1. For the reasons noted above, Appellant submits that claim 1 would not have been obvious to a person of ordinary skill in the art based on the teachings of Le Carpentier and in fact, in many respects as noted above, the Le Carpentier reference teaches away from the subject matter of claim 1.

As to the Liechti et al. reference, which was relied upon as a basis for rejecting certain of the claims depending from claim 1, this reference does, in fact, describe communications between a postage meter and a data center, however, the Examiner did not provide any proposals or indications as to why or how the Examiner believes the teachings of Liechti et al. could be used to modify the procedures described in the Le Carpentier reference. As noted above, many of the data exchanges in the Le Carpentier reference cited by the Examiner do not proceed between the terminal equipment and the local station or the data center, but are in fact data exchanges which take place between the base and franking head at the franking machine. Since the Liechti et al. reference does not describe base/franking head data exchanges in any manner whatsoever, and deals exclusively with data exchanges between a postage meter and a data center, Appellant is unable to

determine why or how the Examiner believes the Liechti et al. teachings could or would be used by a person of ordinary skill in the art to modify the various different types of data exchanges disclosed in the Le Carpentier reference.

Therefore, Appellant respectfully submits that even if the Le Carpentier reference were modified in accordance with the teachings of Liechti et al., the subject matter of claims 2-11, depending from independent claim 1, still would not result. None of claims 1-11, therefore, would have been obvious to a person of ordinary skill in the art based on the teachings of Le Carpentier and Liechti et al.

Independent claim 17 and claims 18-27 depending therefrom are apparatus claims which track method claims 1-11. All of the arguments set forth above with regard to claims 1-11, therefore, apply equally to claims 17-27, and claims 17-27 are submitted to be patentable over the teachings of Le Carpentier and Liechti et al.

As to independent method claim 12, that claim includes the initial step of transmitting unencrypted service data from a data center to terminal equipment. Again the Examiner cited the language at column 5, lines 1-15 as allegedly teaching such a step, in addition to the step of generating a code at the terminal equipment based on the transmitted service data. As noted above, the passage at column 5, lines 1-15 in the Le Carpentier reference refers only to a request being transmitted from the local station to the base 7, in response to which encrypted information is transmitted from the base to the local station. There is nothing in this passage regarding the transmission of service data from a data center to the terminal equipment. Moreover, as noted above although the information transmitted from the base to the local station is encoded or encrypted, there is no teaching in the passage

cited by the Examiner that the encryption is anyway based on the initial request from the local station to the base 7.

Moreover, although the language at column 5, lines 30-33 of the Le Carpentier reference refers to undertaking a parity check of the message that was transmitted from the base 7, it is well-known to those of ordinary skill in the art that a parity check is only for the purpose of determining the internal integrity or correctness of the message which has been transmitted. In other words, a parity check only confirms that the received message is, in fact, the message which was intended to be transmitted. Since, as noted above, the information transmitted from the base 7 to the local station is not in any way dependent on or based on the original request transmitted from the local station to the base 7, the parity check taught in the Le Carpentier reference does not and cannot have any capability of verifying the correctness of the originally transmitted request. In the subject matter of claim 12, by contrast, the code that is generated at the terminal equipment is based on the transmitted service data. Therefore, when this code is transmitted back from the terminal equipment to the data center and the code is checked at the data center, this serves as a verification at the data center of the correct transmittal of the original unencrypted service data. In other words, the check undertaken at the data center does not merely verify a correct (i.e. uncorrupted) transmission of data from the terminal equipment to the data center, but also, since the code is generated dependent on the originally transmitted service data, the check undertaken at the date center simultaneously verifies that this original transmission ensued correctly (i.e., without corruption). No such procedure is disclosed or suggested in the Le Carpentier reference.

Again, since the Examiner cited only passages from the Le Carpentier reference with respect to the language of claim 12, it appears that the Examiner relied only on the Le Carpentier reference as a basis for rejecting claim 12 under 35 U.S.C. §103(a). For the reasons discussed above, Appellant respectfully submits that this rejection is not proper. The claims depending from claim 12 add further steps to the novel and non-obvious combination of claim 12, and are therefore patentable over the teachings of Le Carpentier, even if augmented by the teachings of Liechti et al.

Apparatus claims 28-32 generally track method claims 12-16 and therefore the arguments in support of patentability set forth above with regard to claims 12 and 16 apply equally to claims 28-32. Claims 28-32 therefore are submitted to be allowable over the teachings of Le Carpentier and Liechti et al.

CONCLUSION:

For the foregoing reasons, Appellant respectfully submits the Examiner is in error in law and in fact in rejecting the claims on appeal. Reversal of that rejection is therefore proper, and the same is respectfully requested.

This Appeal Brief is accompanied by the requisite fee in the amount of $320.00.

Submitted by,

Steven H. Noll (Reg. 28,982)

SCHIFF, HARDIN & WAITE
CUSTOMER NO. 26574
Patent Department
6600 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606
Telephone: 312/258-5790
Attorneys for Appellant.

CERTIFICATE OF MAILING

I hereby certify that an original and two copies of this correspondence are being deposited with the United States Postal Service as First Class mail in an envelope addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231 on March 6, 2003.

Steven H. Noll

STEVEN H. NOLL

APPENDIX "A"

1. A method for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising the steps of:

offering new service data at a data center for future use at terminal equipment;

forming a request for new service data at the terminal equipment;

establishing a first communication between the terminal equipment and the data center and in said first communication transmitting said request data from the terminal equipment to the data center, receiving the request data at the data center, transmitting the new service data requested in the request data from the data center to the terminal equipment, and receiving and storing the new service data at the terminal equipment; and

establishing a second communication between the terminal equipment and the data center and in said second communication forming a message at the terminal equipment that refers to the new service data stored at the terminal equipment, communicating said message from the terminal equipment to the data center, receiving the message from the terminal equipment at the data center and checking the message at the data center by comparison of information contained in the message with information generated from the new service data at the data center and, given a positive comparison result, transmitting a follow-up message from the data center to the terminal equipment allowing said

terminal equipment, when appropriate, to use said new service data, and registering at the data center the valid transmission of the new service data to the terminal equipment.

2. A method as claimed in claim 1 wherein said follow-up message comprises an OK message allowing the terminal equipment to be switched into an operating mode.

3. A method as claimed in claim 2 wherein the step of transmitting said OK message includes transmitting a marking in said OK message indicating that the new service data stored at the terminal equipment are valid.

4. A method as claimed in claim 1 wherein the step of storing the new service data in the first communication comprises intermediately storing the new service data at the terminal equipment, and wherein the step of transmitting said follow-up message in said second communication comprises transmitting a load instruction from the data center to the terminal equipment, and wherein said second communication includes the step of, upon receipt of said load instruction at the terminal equipment, loading the new service data into a non-volatile memory of a processing module at the terminal equipment.

5. A method as claimed in claim 1 wherein the step of forming said message in the second communication at the terminal equipment comprises forming a message including a version number associated with the new service data and a checksum.

6. A method as claimed in claim 1 wherein the step of forming said message in the second communication at the terminal equipment comprises forming

a message including a version number associated with the new service data and an encrypted checksum.

7. A method as claimed in claim 1 wherein the step of offering said new service data comprises offering postage fee schedule table data as said new service data, and comprising the step of providing a postage computer having a processing module which makes use of said postage fee schedule table data at said terminal equipment.

8. A method as claimed in claim 7 wherein the step of forming said message in said second communication at said terminal equipment includes forming a message including a version number of the new service data and an encrypted checksum, and comprising the step of providing a postage meter machine at said terminal equipment in communication with said postage computer, storing a secret key in said postage meter machine, forming said encrypted checksum in said postage meter machine using a symmetrical encryption algorithm and said secret key, and storing said secret key as well at said data center and using said secret key at said data center to check said message from said terminal equipment in said second communication.

9. A method as claimed in claim 7 wherein the step of forming said message in said second communication at said terminal equipment comprises forming a message including a version number of the new service data and an encrypted checksum, and comprising the steps of storing a public key in said postage computer and forming said encrypted checksum in said postage computer using an asymmetrical encryption algorithm and said public key, and storing a non-public secret key, related to said public key, at said data center and using said non-

public secret key at said data center to check said message in said second communication.

10. A method as claimed in claim 1 wherein the step of offering new service data at said data center comprises offering new postage fee schedule table data at said data center for future use in postage calculation, and wherein the step of checking the message transmitted from the terminal equipment to the data center in the second communication comprises checking information contained in said message by comparison with information generated from the new postage fee schedule table data, and wherein the step of transmitting said follow-up message in said second communication from said data center to the terminal equipment comprises transmitting an OK message indicating that the new postage fee schedule table data received at said terminal equipment are valid and also including a load instruction instructing the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of a postage computer at said terminal equipment.

11. A method as claimed in claim 10 comprising the additional step of loading said new postage fee schedule table data into said non-volatile memory at said postage computer upon receipt at said terminal equipment of said follow-up message.

12. A method for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising the steps of:

transmitting unencrypted service data from a data center to terminal equipment;

generating a code at the terminal equipment based on the transmitted service data;

transmitting said code from said terminal equipment to said data center; and

receiving said code at said data center and checking said code at said data center and transmitting a message from said data center to said terminal equipment identifying a result of the check.

13. A method as claimed in claim 12 comprising providing a postage computer at said terminal equipment, and wherein the step of transmitting unencrypted service data to the terminal equipment comprises transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and comprising the steps of generating a checksum at said postage computer based on the transmitted fee schedule table data and transmitting the checksum to the data center as at least a part of said code, and wherein the step of checking the code at the data center comprises checking the checksum at the data center on the basis of a stored checksum stored at said data center and wherein the step of transmitting a message to the terminal equipment comprises transmitting an OK message to the terminal equipment given coincidence of said stored checksum with the checksum transmitted to the data center.

14. A method as claimed in claim 12 comprising providing a postage computer at said terminal equipment, and wherein the step of transmitting unencrypted service data to the terminal equipment comprises transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and comprising the steps of generating a encrypted code at said postage computer based on the transmitted fee schedule table data and transmitting

the encrypted code to the data center as at least a part of said code, and wherein the step of checking the code at the data center comprises checking the encrypted code at the data center on the basis of a stored encrypted code stored at said data center and wherein the step of transmitting a message to the terminal equipment comprises transmitting an OK message to the terminal equipment given coincidence of said stored encrypted code with the encrypted code transmitted to the data center.

15. A method as claimed in claim 12 comprising providing a postage computer at said terminal equipment and wherein the step of transmitting unencrypted service data to the terminal equipment comprises transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein the step of generating a code at the terminal equipment comprises generating a signature representing information dependent on the transmitted fee schedule table data and encrypting said information with a public write key to form said signature, and wherein the step of transmitting said code to the data center comprises transmitting said signature to the data center, and wherein the step of checking the code at the data center comprises decrypting the signature at the data center with a secret read key according to an asymmetrical algorithm and checking the information in the signature with information stored at the data center and, given a positive comparison result, transmitting an OK message to the terminal equipment.

16. A method as claimed in claim 15 comprising the step of forming a checksum as said information contained in said signature.

17. An arrangement for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising:

a data center, and terminal equipment located remote from said data center, said data center offering new service data for future use at said terminal equipment;

means for forming a request for new service data at the terminal equipment;

means for establishing a first communication between the terminal equipment and the data center and in said first communication transmitting said request data from the terminal equipment to the data center, means for receiving the request data at the data center and for transmitting the new service data requested in the request data from the data center to the terminal equipment, and means for receiving and storing the new service data at the terminal equipment; and

means for establishing a second communication between the terminal equipment and the data center and in said second communication forming a message at the terminal equipment that refers to the new service data stored at the terminal equipment and for communicating said message from the terminal equipment to the data center, means for receiving the message from the terminal equipment at the data center and for checking the message at the data center by comparing information contained in the message with information generated from the new service data at the data center and, given a positive comparison result, for forming and transmitting a follow-up message from the data center to the terminal equipment allowing said terminal equipment, when appropriate, to use said new service data, and

means for registering at the data center the valid transmission of the new service data to the terminal equipment.

18. An arrangement as claimed in claim 17 wherein said means for forming said follow-up message comprises means for forming an OK message allowing the terminal equipment to be switched into an operating mode.

19. An arrangement as claimed in claim 18 wherein said means for forming said OK message means for including a marking in said OK message indicating that the new service data stored at the terminal equipment are valid.

20. An arrangement as claimed in claim 17 wherein said means for storing the new service data in the first communication comprise means for intermediately storing the new service data at the terminal equipment, and wherein said means for transmitting said follow-up message in said second communication comprise means for transmitting a load instruction from the data center to the terminal equipment, and wherein said terminal equipment comprises means for, upon receipt of said load instruction at the terminal equipment, loading the new service data into a non-volatile memory of a processing module at the terminal equipment.

21. An arrangement as claimed in claim 17 wherein said means for forming said message in the second communication at the terminal equipment comprise means for forming a message including a version number associated with the new service data and a checksum.

22. An arrangement as claimed in claim 17 wherein said means for forming said message in the second communication at the terminal equipment comprise means for forming a message including a version number associated with the new service data and an encrypted checksum.

23. An arrangement as claimed in claim 17 wherein said data center comprises means for offering postage fee schedule table data as said new service data, and wherein said terminal equipment comprises a postage computer having a processing module which makes use of said postage fee schedule table data.

24. An arrangement as claimed in claim 23 wherein said means for forming said message in said second communication at said terminal equipment comprise means for forming a message including a version number of the new service data and an encrypted checksum, and wherein said terminal equipment comprises a postage meter machine in communication with said postage computer, means for storing a secret key in said postage meter machine, means for forming said encrypted checksum in said postage meter machine using a symmetrical encryption algorithm and said secret key, and wherein said data center comprises means for storing said secret key as well at said data center and wherein said means for checking comprise means for using said secret key to check said message from said terminal equipment in said second communication.

25. An arrangement as claimed in claim 23 wherein said means for forming said message in said second communication at said terminal equipment comprise means for forming a message including a version number of the new service data and an encrypted checksum, and wherein said postage computer comprises means for storing a public key and for forming said encrypted checksum using an asymmetrical encryption algorithm and said public key, and wherein said data center comprises means for storing a non-public secret key, related to said public key, at said data center and wherein said means for checking comprise means for using said non-public secret key to check said message in said second communication.

26. An arrangement as claimed in claim 17 wherein said data center comprises means for offering new postage fee schedule table data at said data center for future use in postage calculation, and wherein said means for checking the message transmitted from the terminal equipment to the data center in the second communication comprises means for checking information contained in said message by comparison with information generated from the new postage fee schedule table data, and wherein said means for transmitting said follow-up message in said second communication from said data center to the terminal equipment comprises means for transmitting an OK message indicating that the new postage fee schedule table data received at said terminal equipment are valid and also including a load instruction instructing the terminal equipment to load the new postage fee schedule table data into a non-volatile memory of a postage computer at said terminal equipment.

27. An arrangement as claimed in claim 26 wherein said terminal equipment comprises loading said new postage fee schedule table data into said non-volatile memory at said postage computer upon receipt at said terminal equipment of said follow-up message.

28. An arrangement for dependably transmitting service data from a data center to remotely-located terminal equipment, comprising:

a data center, and terminal equipment located remote from said data center;

means for transmitting unencrypted service data from the data center to the terminal equipment;

means for generating a code at the terminal equipment based on the transmitted service data;

means for transmitting said code from said terminal equipment to said data center; and

means for receiving said code at said data center and for checking said code at said data center and for transmitting a message from said data center to said terminal equipment identifying a result of the check.

29. An arrangement as claimed in claim 28 wherein said terminal equipment comprises a postage computer, and wherein said means for transmitting unencrypted service data to the terminal equipment comprises means for transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein said postage computer comprises means for generating a checksum based on the transmitted fee schedule table data and wherein said means for transmitting said code comprise means for transmitting the checksum to the data center as at least a part of said code, and said means for checking the code at the data center comprise means for checking the checksum at the data center on the basis of a stored checksum stored at said data center and for transmitting a message to the terminal equipment comprising an OK message to the terminal equipment given coincidence of said stored checksum with the checksum transmitted to the data center.

30. An arrangement as claimed in claim 28 wherein said terminal equipment comprises a postage computer, and said means for transmitting unencrypted service data to the terminal equipment comprises means for transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein said postage computer comprises means for generating a encrypted code based on the transmitted fee schedule table data and

wherein said means for transmitting said code comprise means for transmitting the encrypted code to the data center as at least a part of said code, and wherein said means for checking the code at the data center comprise means for checking the encrypted code at the data center on the basis of a stored encrypted code stored at said data center and for transmitting a message to the terminal equipment comprising an OK message to the terminal equipment given coincidence of said stored encrypted code with the encrypted code transmitted to the data center.

31. An arrangement as claimed in claim 28 wherein said terminal equipment comprises a postage computer and wherein said means for transmitting unencrypted service data to the terminal equipment comprise means for transmitting unencrypted fee schedule table data, as said unencrypted service data, to said postage computer, and wherein said postage computer comprises said means for generating a code at the terminal equipment, said postage computer generating a signature, as said code, representing information dependent on the transmitted fee schedule table data and encrypting said information with a public write key to form said signature, and wherein said means for transmitting said code to the data center comprises means for transmitting said signature to the data center, and said means for checking the code at the data center comprise means for decrypting the signature at the data center with a secret read key according to an asymmetrical algorithm and for checking the information in the signature with information stored at the data center and, given a positive comparison result, for transmitting an OK message to the terminal equipment.

32. An arrangement as claimed in claim 31 wherein said postage computer comprises forming a checksum as said information contained in said signature.